CLAIMS

1. A method of automatically classifying alerts issued by intrusion detection sensors (11a, 11b, 11c) of an information security system (1) for producing collated alerts, each alert being defined by a plurality of qualitative attributes $(a_1,...,a_n)$ belonging to a plurality of attribute domains $(Al,...,An)$ each of which has a partial order relationship, which method is characterized in that it comprises the following steps:

· organizing the attributes belonging to each attribute domain into a hierarchical structure including levels defined in accordance with the partial order relationship of the attribute domain, the attribute domains thus forming hierarchical structures;

· constructing for each alert issued by the intrusion detection sensors (11a, 11b, 11c) a trellis specific to that alert by generalizing each alert in accordance with each of its attributes and at all the levels of the hierarchical structure, the specific trellis including nodes corresponding to alerts linked to each other by arcs so that each node is linked to one or more parent nodes and/or to one or more child or descendant nodes;

· iteratively merging each specific trellis into a general trellis;

· identifying collated alerts in the general trellis by selecting the alerts that are simultaneously the most pertinent and the most general in accordance with statistical criteria and according to their attributes belonging to lower levels of the hierarchical structures; and

· supplying the collated alerts to an output unit (23) of an alert management system (13) in order to provide an overview of all the alerts issued by the intrusion detection sensors (11a, 11b, 11c).

2. A method according to claim 1, characterized in that the construction of a specific trellis includes the following steps:

· for any generalizable attribute of a given alert, recovering the generalized value of that attribute from its hierarchical structure to form a new alert more general than said given alert;

· adding a new node to the specific trellis corresponding to the new alert and adding an arc going from the new node of the new alert to the node of the given alert; and

· adding missing arcs going from the parent nodes of the given alert resulting from the generalization of the given alert in accordance with its other attributes to the node of the new alert.

3. A method according to either claim 1 or claim 2, characterized in that merging a given specific trellis into the general trellis includes the following steps:

· selecting a first node corresponding to a first alert belonging to the given specific trellis and a second node corresponding to a second alert belonging to the general trellis;

· eliminating all the arcs coming from the parent nodes of an offspring node of the first node if said offspring node belongs to said general trellis; and

· adding said offspring node and all its descendants to the general trellis if said offspring node does not belong to the general trellis.

4. A method according to any one of claims 1 to 3, characterized in that a pertinent alert is identified when each of the sets of offspring nodes of the pertinent alert resulting from specialization of that alert in accordance with each of its attribute domains is homogeneous and when the number of elements constituting

each of said sets of offspring nodes of the pertinent alert is greater than a threshold value.

5. A method according to any one of claims 1 to 4, characterized in that the collated alerts are associated with different groups of alerts issued by the sensors so that the groups are not mutually exclusive.

6. A method according to any one of claims 1 to 5, characterized in that the attribute domains include domains from the following sets: alert identifiers, attack sources, attack targets, and attack dates.

7. A computer program characterized in that it is designed to execute the method according to any one of claims 1 to 6 when it is executed by the alert management system (13).